

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

平1-181349

⑤ Int. Cl.<sup>4</sup>

識別記号

庁内整理番号

⑬ 公開 平成1年(1989)7月19日

H 04 L 9/02  
1/00  
11/00

3 1 0

Z-7240-5K  
B-8732-5K  
Z-7928-5K

審査請求 未請求 請求項の数 4 (全7頁)

⑭ 発明の名称 同報通信システム

⑮ 特 願 昭63-6586

⑯ 出 願 昭63(1988)1月14日

⑰ 発 明 者 柳 宏 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内  
⑱ 発 明 者 木 原 洋 一 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内  
⑲ 出 願 人 日本電信電話株式会社 東京都千代田区内幸町1丁目1番6号  
⑳ 代 理 人 弁理士 玉蟲 久五郎 外2名

明 細 書

1. 発明の名称

同報通信システム

2. 特許請求の範囲

(1) 通信要求発生の際暗号キーを生成し、個別接続形伝達路を経由して該暗号キーを加入者番号に対応する加入者に送達する手段と、情報を該暗号キーで暗号化し誤り訂正符号を付加し暗号化情報を形成し、これを放送形伝達路を経由して受信端末に一齐に放送的に伝達する手段とを有する情報出力装置と、

前記個別接続形伝達路を経由して受信した暗号キーと、前記放送形伝達路を経由して受信した前記暗号化情報とより元情報を復号する前記受信端末よりなることを特徴とする同報通信システム。

(2) 複数の加入者番号から成る同報宛先と同報に使用する元情報を、同報要求端末から前記個別接続形伝達路を経由して前記情報出力装置に送達する手段とを備えたことを特徴とする特許請求の範囲

第1項記載の同報通信システム。

(3) 前記受信端末は、前記誤り訂正符号の誤り訂正が正常に行われた時に、自加入者番号と正しく受信できたことを通知する受信確認信号を前記個別接続形伝達路を経由して情報出力装置に返送する手段を備えたことを特徴とする特許請求の範囲第1項記載の同報通信システム。

(4) 同報要求端末からの同報通信要求の受付ならびに前記受信端末から前記情報出力装置に返送されてきた加入者番号の一覧から成る同報通信状況の報告を、前記個別接続形伝達路を経由して同報要求端末に送達する手段を備えたことを特徴とする特許請求の範囲第1項記載の同報通信システム。

3. 発明の詳細な説明

(産業上の利用分野)

本発明はデータ通信に関するものであつて、特に、無線伝達路あるいは多重接続機能を有する有線伝達路を用いた同報通信システムに関する。

## 特開平1-181349 (2)

## 〔従来の技術〕

第2図は従来の同報通信システムの個別接続形伝達路のブロック図である。図において、1は情報出力装置、2は個別接続形伝達路、3は受信端末である。

従来、同一の情報を複数の特定加入者に送信する同報通信システムにおいては、

(1) 有線等の個別接続形伝達路2で受信端末3と情報出力装置1を1対1に接続した後、情報の送信処理を行い、これらの動作を順次送信先の受信端末の数だけ繰り返すことにより同報通信を実現していた。

(2) 無線のような放送形伝達路を用いて同報通信を実現していた。

## 〔発明が解決しようとする課題〕

この(1)の方式では、以下の欠点がある。

①宛先端末ごとに逐次回線接続と送信処理が必要となるため、端末間で情報を受信する時間差が生ずる。

## 〔実施例〕

(1) 第1図は本発明のシステムのブロック図、第3図は本発明の詳細なブロック図である。

1は情報出力装置、3は受信端末、4は情報、5は宛先、6は伝達確認手段、7は暗号キー生成手段、8は暗号化手段、9は誤り訂正符号付加手段、10は放送形伝達路送信手段、11は個別接続形伝達路送受信手段、12は個別接続形伝達路、13は放送形伝達路、14は同報要求端末、15は個別接続形伝達路送受信手段、20は個別接続形伝達路送受信手段、23は放送形伝達路送信手段、24は誤り訂正手段、25は暗号復号化手段を示す。

## ①本処理

情報出力装置1は暗号キー生成手段7で通信要求発生の都度暗号キーを生成し、個別接続形伝達路送受信手段11で個別接続形伝達路12を経由して宛先5で加入者番号(以下DN(Directory Number)と略す)に対応して指定された複数の受信端末3毎に該暗号キーを逐次

②時間差を少なくするためには、情報出力装置1と伝達路の途中に入る交換装置の間の回線数を増加し、さらに情報出力装置1の処理能力を向上させる必要がある。

③このため、システムが高価なものとなる。

一方、(2)の方式では、前述の問題は無くなるが、

①受信端末3を特定できない、

②通信方向が片方向であり、通信内容が受信端末側に正しく届いたか否かの確認(送達確認)が出来ない。

③第3者に通信内容が漏れてしまう。

等の問題点が発生する。

## 〔課題を解決するための手段〕

本発明は情報出力装置から受信端末に個別接続形伝達路と放送形伝達路との2つの伝達路を設け、個別接続形伝達路により復号化のための暗号キーの伝達ならびに送達確認の連絡を行い、放送形伝達路により同報情報の伝達を行うようにした。

送信する。

一般に、暗号キーのデータ長は、暗号化される元情報のデータ長より充分小さくできるので、暗号キーの逐次送信に要する時間及び処理負荷は極めて小さい。

一方、情報出力装置1は暗号化手段8で前記暗号キーを用いて同報要求端末より受けた同報要求の元情報を該暗号キーで暗号化し、これに誤り訂正符号付加手段9で誤り訂正符号を付加して暗号化情報を形成した後、放送形伝達路送信手段10で放送形伝達路13を経由して不特定多数の受信端末3に対し、放送により一斉に送信する。受信端末3は、この暗号化情報を受信し、誤り訂正手段24で伝送時の伝送誤りを訂正し、先に別途受信していた暗号キーを用いて暗号化情報から暗号復号化手段25により復号化する。

## ②同報要求処理

同報要求を行う同報要求端末14は個別接続形伝達路送受信手段15で、同報通信先である複数のDNから成る送信宛先と、元情報とを個別接続

## 特開平1-181349 (3)

形伝達路12を経由で情報出力装置1に送信する。

## ④受信確認処理

受信端末3は誤り訂正が正常に行われたことを確認した時、個別接続形伝達路送受信手段20は自DNを付加した受信確認信号を個別接続形伝達路12経由で情報出力装置1に返送する。

## ④同報通信状況処理

情報出力装置1はこの受信確認信号を受信し、送達確認手段6で前記受信確認信号に付加されていたDNと同報宛先のDNを比較して同報通信状況を算出する。すなわち、前記受信確認信号のDNから送達確認ができ、同報宛先のDNに含まれた前記受信確認信号のDNに含まれないDNから不達確認ができる。これにより、情報出力装置1は個別接続形伝達路送受信手段11で前記同報通信状況を同報要求端末14に報告し、同報要求端末14はその同報通信状況を受信する。

以上説明したように、本発明によれば、放送形伝達路13を用いて一斉に情報伝達が行われるために、個別接続形伝達路12を用いた場合より安

価で、受信端末3の間で情報受信時間差のない同報通信が実現できる。

放送形伝達路13で放送される暗号化された情報は、同報宛先以外の受信端末も受信可能であるが、暗号化されているので、第3者に通信内容が漏れる心配はない。また、個別接続形伝達路12を用いて受信確認信号を情報出力装置1に返送できるので、送達確認ができる。

この様に、受信端末3に個別接続形伝達路12に放送形伝達路13の2つの伝達路を組合せ、夫々の長所を生かせるシステムが構築できる。

(2) 第4図は本発明の1つの実施例のシステムブロック図で、時分割多重スイッチにより多重接続する機構（以下マルチバス機構と略す）を有する通信制御部39対応のデジタル交換装置31を伝達路に用いた例である。図において、31はデジタル交換装置（マルチバス接続機構）、32はCPU、33は端末要求受付処理部、34は乱数発生部、35は暗号化処理部、36は蓄積部、38はRAM、39は通信制御部、40は誤り訂

正符号処理部、41は受信確認信号処理部、42はROMである。デジタル交換装置31はISDN対応のマルチバス接続機構を持ち、通信制御部39はISDN基本インタフェース(2B+D)通信制御部であり、多重化された2個のBch回線と1個のDchパケットに対する送受信制御を行う。第4図の各ブロックは情報出力装置1、同報要求端末14、受信端末3の構成ブロックが何れも電算機と略同一構成なことを示した。第1図における個別接続形伝達路12および放送形伝達路13は、本実施例では、マルチバス接続機構を有するデジタル交換装置31に縮退しており、個別接続形伝達路12はDchパケットを用い、た伝達路に、放送形伝達路13はBchのマルチバス接続機構を用いた伝達路に夫々対応する。まず最初に、1本のデータハイウェイに3本の端末回線が多重化されている例のマルチバス接続機構について説明する。多重度は3以上でも動作原理は同じである。

第5図はデジタル交換装置31におけるマル

チバス接続の原理の説明図である。図において、51はタイムスロットメモリ、52は読み出し制御メモリ、53はクロック、54は入データハイウェイ、55は出データハイウェイである。タイムスロットメモリ51によるデジタル交換動作の概要をまず説明する。複数の端末回線から入力されるデジタル信号は、タイムスロットと呼ばれる一定の長さのデータに区切られ、入データハイウェイ54において各端末回線に1対1に対応するタイムスロットとして多重化されて運ばれる。同様にデータハイウェイ55の上で多重化されて運ばれる各タイムスロット上の信号は、夫々対応する端末回線へ分配して送信される。A、B、Cは、夫々端末回線#1、端末回線#2、端末回線#3から入力されてデータハイウェイ上に多重化されて転送されるタイムスロット上の信号を表す。クロック53はタイムスロットメモリ51の書き込みをタイムスロット単位で行うタイミング及び読み出し制御メモリ52を読み出すタイミングを供給するためのものである。タイムスロットメモ

## 特開平1-181349 (4)

リ51は、入データハイウェイ54から入力されるタイムスロットを順番にタイムスロットメモリ51に書き込んでいく。一方、読み出し制御メモリ52は、タイムスロットメモリ51に書き込まれたタイムスロットを読み出す順番を記憶するためのメモリである。読み出し制御メモリ52の内容を変更することにより、タイムスロットメモリ51に書き込まれた順番と異なる順番でタイムスロットを読み出し、出データハイウェイ55へ送出することが可能となり、入データハイウェイ54と出データハイウェイ55とでタイムスロットの順序が変わり、端末回線間の信号の交換が可能となる。

次に、以上説明したデジタル交換装置31を使ったマルチバス接続機構を説明する。第5図において、読み出し制御メモリ52の内容を、例えばすべて2にしておくと、出データハイウェイ55上には全てBが読み出され、すべての端末回線にBが送出されることになるので、マルチバス接続機構が実現できる。端末回線#2から入力され

た信号をタイムスロットメモリ51から#1、#2、#3の各端末回線に送出する時間差は、端末回線上においてタイムスロット1個を送信するのに要する時間以下である。通常のデジタル交換装置31における交換処理の単位であるタイムスロットは、数ビットの長さしかなく、同報送信する全体の情報の長さに比してはるかに小さいので、本マルチバス接続機構による同報時間差は事実上無視でき、放送形伝達路と同等の機能を持つものと考えられる。

次に本実施例の動作を説明する。

## ①本処理

第6図は実施例の動作概要の流れ図である。

同報送信に先立ち、種々の同報通信要求で選択される可能性のある全ての受信端末3と情報出力装置1をマルチバス接続できるように、デジタル交換装置31の読み出し制御メモリ52の内容は、前述した方法で事前に設定しておく。すなわち、前記マルチバス接続機構により、受信端末3のBch回線が空きの状態のときには、該Bch回線

を情報出力装置1のBch回線に接続されるようにしておくようにする。これにより、情報出力装置1およびデジタル交換装置31は、情報出力装置1とDNで指定される受信端末3との間の接続処理を同報呼の生起する毎に行わずに、情報出力装置1からの送信情報を、時間差なく、マルチバス接続された全ての受信端末3に送出することが可能となる。従つて、従来の同報通信システムが1対1の接続を逐次あるいは複数回線を使っていたのに比較して、接続および情報送信の処理負荷が格段に低減し、また、情報出力装置1側の回線が1回線のみですむので、はるかに経済的なシステムとなる。この効果は、同報の宛先数が多くなるほど顕著である。

この様な状況で同報通信要求が発生すると、まず、情報出力装置1は乱数を発生し、暗号キーとする。この暗号キーを同報宛先5で指定される受信端末3に対し、Dchパケットで順次送信していく。受信端末3は暗号キーを受信するとともに、Bchを他の端末が使用しないように閉塞する。

情報出力装置1は、前記暗号キーで送信の元情報を暗号化し、誤り訂正符号を付加して暗号化情報を形成し、Bch経由でデジタル交換装置31に送出する。デジタル交換装置はマルチバス接続機構で、同報宛先に無関係に不特定の受信端末に対し情報出力装置1から受けた情報をBchを用いて送出する。受信端末3はBchで受信した暗号化情報の誤り訂正を行い、前記方法で受信した暗号キーで復号する。

## ②同報要求処理

まず同報要求端末14は同報送信を依頼する情報と同報宛先をDchパケットを用いて情報出力装置1に送出する。情報出力装置1は同報要求端末14からの送信情報と同報宛先を受信する。以後の動作は前述のとおりである。

## ③受信確認処理

受信端末3は誤り訂正が正しく行われた時点で、Dchパケットを用いて情報出力装置1に受信確認信号を返送する。Dchパケットは発信者識別番号が自動的に付加されるため、受信確認信号に

## 特開平1-181349 (5)

は受信端末3のDNが付加されている。また、受信端末3が受信確認信号返送時に使用する情報出力装置1のDNは、暗号キー受信時入力Dchパケットに付加されてくる発信者識別番号を用いればよい。情報出力装置1は受信確認信号を受信し、受信確認信号に付加されているDNから正しく通信できた受信端末3を知り、同報宛先と比較することで正しく通信できなかった受信端末3を知ることができる。

## ④同報通信状況処理

情報出力装置1は正しく通信できた受信端末3のDN及び正しく通信できなかった受信端末3のDNの一覧から成る同報通信状況を、Dchパケットを用いて同報要求端末14に送出する。

## 〔発明の効果〕

本発明によれば、個別接続形伝送路と放送形伝送路を組合せることで、第3者に通信内容が漏れることのない、送達確認が可能な、端末間で受信時間差のない経済的な同報通信システムを提供す

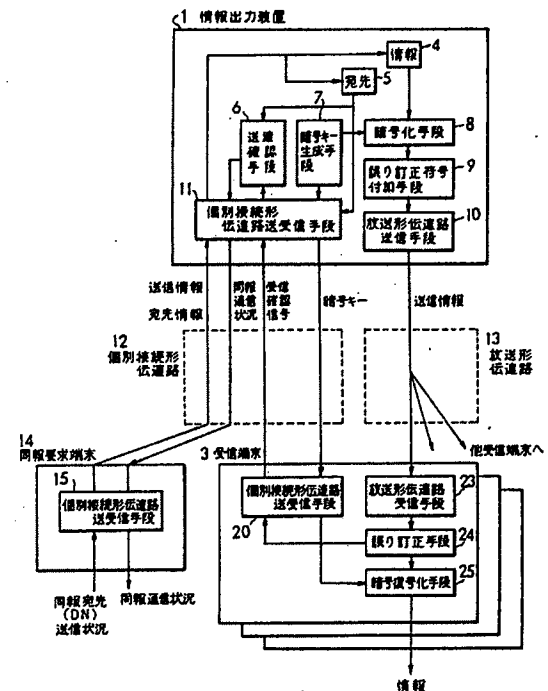
ることができる。

## 4.図面の簡単な説明

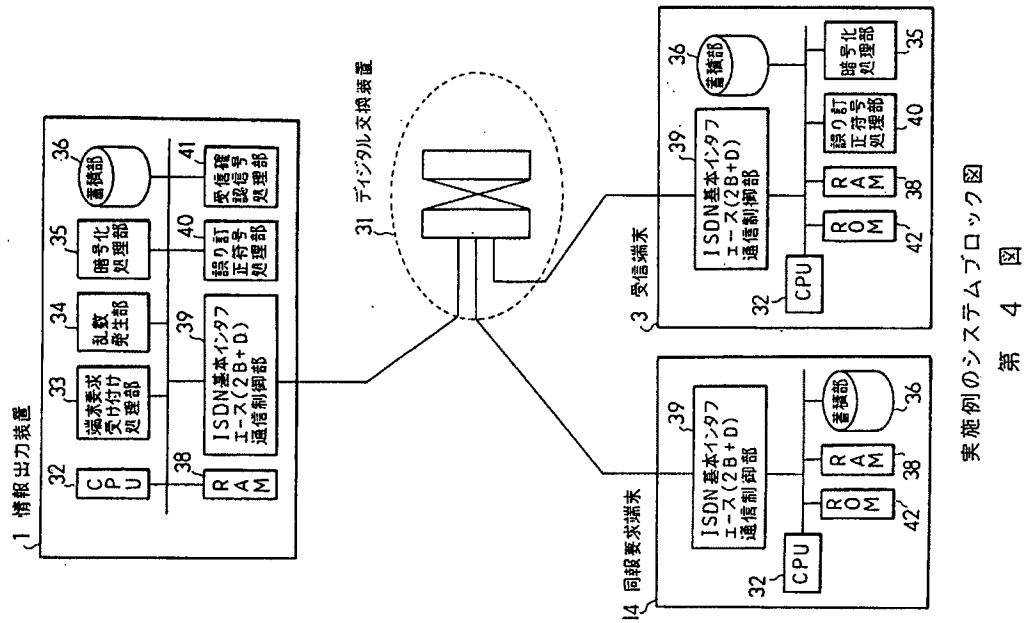
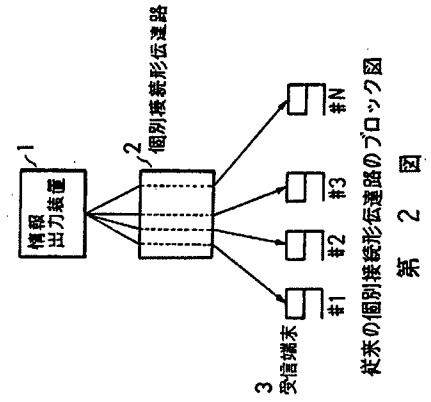
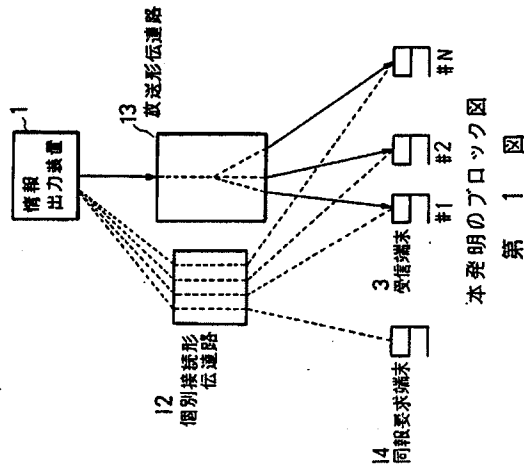
第1図は本発明のシステムのブロック図、第2図は従来の同報通信システムの個別接続形伝送路のブロック図、第3図は本発明の詳細なブロック図、第4図は本発明の1つの実施例のシステムブロック図、第5図はデジタル交換装置のマルチバス接続の原理の説明図、第6図は実施例の動作概要の流れ図である。

1は情報出力装置、2は個別接続形伝送路、3は受信端末、4は情報、5は宛先、6は送達確認手段、7は暗号キー生成手段、8は暗号化手段、9は誤り訂正符号付加手段、10は放送形伝送路送信手段、11は個別接続形伝送路送受信手段、12は個別接続形伝送路、13は放送形伝送路、14は同報要求端末、15は個別接続形伝送路送受信手段、20は個別接続形伝送路送受信手段、23は放送形伝送路送信手段、24は誤り訂正手段、25は暗号復号化手段、

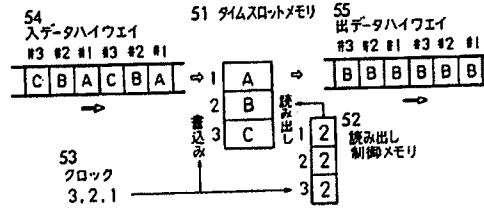
31はデジタル交換装置、32はCPU、33は端末要求受付処理部、34は乱数発生部、35は暗号化処理部、36は蓄積部、38はRAM、39は通信制御部、40は誤り訂正符号処理部、41は受信確認信号処理部、42はROM、51はタイムスロットメモリ、52は読み出し制御メモリ、53はクロック、54は入データハイウェイ、55は出データハイウェイ、DNは加入者番号。



特許出願人 日本電信電話株式会社  
代理人 弁理士 玉 蟲 久五郎  
(外2名)

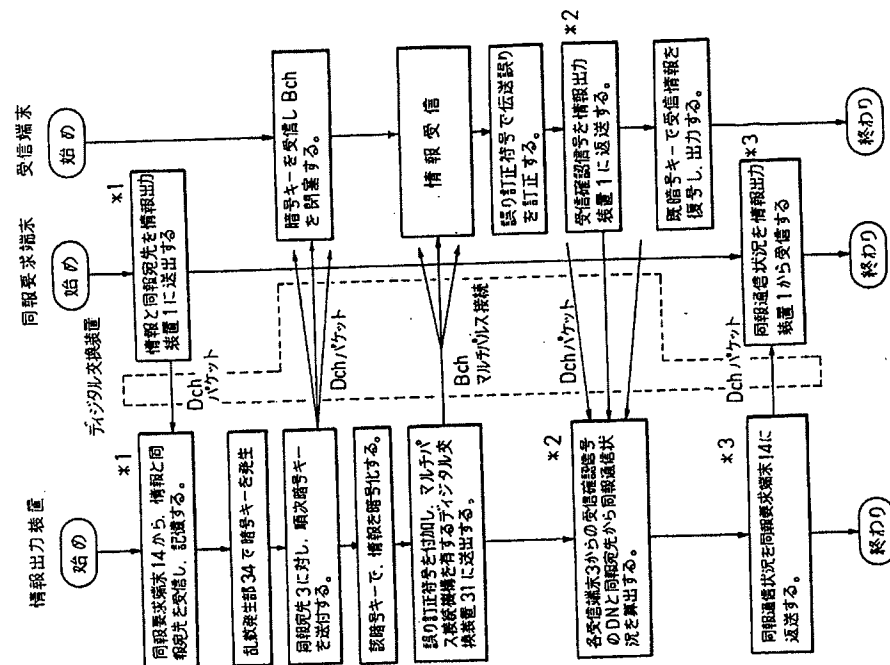


特開平1-181349 (7)



マルチパス接続の原理の説明図

第 5 図



注) \*1: 特許請求範囲第3項及び第4項において追加される動作  
 \*2: 特許請求範囲第2項において追加される動作  
 \*3: 特許請求範囲第4項において追加される動作

実施例の動作概要の流れ図

第 6 図

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-181349

(43)Date of publication of application : 19.07.1989

---

(51)Int.Cl. H04L 9/02  
H04L 1/00  
H04L 11/00

---

(21)Application number : 63-006586 (71)Applicant : NIPPON TELEGR & TELEPH  
CORP <NTT>

(22)Date of filing : 14.01.1988 (72)Inventor : YANAGI HIROSHI  
KIHARA YOICHI

---

## (54) MULTIPLE ADDRESS COMMUNICATION SYSTEM

### (57)Abstract:

PURPOSE: To obtain an economical multiple address communication system where the content of communication is not leaked to a 3rd party and there is no reception time difference between terminal equipments enabling the confirmation of transmission by combining an individual connection type transmission line and a broadcast type transmission line.

CONSTITUTION: Two transmission lines of individual connection type transmission line 12 and broadcast type transmission line 13 are provided from an information output device 1 to a reception terminal equipment 3. Then the transmission of a cryptographic key for decoding and the communication of transmittal confirmation are applied through the individual connection type transmission line 12 and the multiple address information is sent through the broadcast type transmission line 13. Thus there is no care about the leakage of the content of communication to the 3rd party and the transmission is confirmed and the inexpensive multiple address communication system is obtained where there is no reception time difference between terminal equipments.